Department of Public Health's Covered Entity Status Under HIPAA

The Massachusetts Department of Public Health (Department) declared itself a hybrid entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This determination was made after a thorough analysis of the many and varied programs at the Department.

As a hybrid entity under HIPAA, the Department as a whole is considered a covered entity whose business activities include both covered and non-covered functions. In compliance with 45 CFR §164.105 (a)(2)(iii)(C), the Department designated the following programs as covered health care components within the hybrid entity:

1. Childhood Lead Screening Laboratory
2. The DPH Hospitals
   - Lemuel Shattuck Hospital
   - Massachusetts Hospital School
   - Tewksbury Hospital
   - Western Massachusetts Hospital
   - State Office of Pharmacy Services
3. Services that involve PHI, which are provided to the above-listed covered components by:
   - Office of General Counsel;
   - Accounting;
   - Hospital Bureau; and
   - Quality control and technical services provided by the State Laboratory Institute specifically in support of the Childhood Lead Screening Laboratory.

The Department included in its covered health care components those programs that would meet the definition of a covered entity[1] if each were a separate legal entity. This list could change in the future if certain business practices change. This means that only the above-listed programs are required to comply with the Privacy and Security Rules under HIPAA. Nonetheless, the Department has implemented confidentiality and security policies department-wide that incorporate many of the HIPAA standards.

[1] 45 CFR § 160.103 (definition of covered entity)

Determining that the Department is a hybrid entity also means that the release of PHI from a covered component to a non-covered component is considered a disclosure under HIPAA and is not permitted unless there is an individual authorization or a specific exemption allowing the disclosure. The Privacy Rule requires the Department to implement protections between the covered and non-covered components to assure that PHI is not improperly disclosed.

The Department is aware of a number of questions related to its hybrid status. First, there may be confusion about why certain programs were included as covered components and why other programs, which look like they should be covered as providers or health plans, were not. Many of the Department's programs that contract for the provision of health care are not required to be in the covered component because they do not transmit health information in electronic form in connection with one of the standard transactions specified in the regulations[2]. Other programs that pay for health care were excluded as health plans under the exclusion in the regulations for government funded programs[3].

Second, vendors, as well as licensees and other entities that report PHI to the Department, may have concerns regarding the implications of the hybrid status in relation to reporting or disclosing PHI to the Department. In general, there should be no change in the ability of covered entities to disclose PHI to either the covered or non-covered components of the Department.

It is important to note that the HIPAA statute[4] provides that it was not intended to interfere with the implementation of state public health laws and programs. Vendors that contract with the Department are authorized to continue to disclose PHI to the Department for payment purposes as well as pursuant to the terms and conditions of their contracts, the requirements of which are authorized by state regulations. Licensees are required or authorized by law to provide to the Department access to PHI for health oversight, inspections, and complaint investigations. Other entities are similarly required or authorized by law to report specific PHI to the Department. Outlined below are numerous provisions that permit the continued disclosure of PHI to the Department:

- HIPAA allows a covered entity to disclose PHI to the Department if such disclosure is required by law[5]. (§164.512(a))

- HIPAA allows a covered entity to disclose PHI to a public health authority, or to an agent of a public health authority, when the public health authority is authorized by law to collect or receive such information, for the purpose of preventing or controlling disease, injury, or disability. This includes, but is not

[2] 45 CFR §160.103 (definition of transaction)
[3] 45 CFR §160.103 (definition of health plan)
[4] P.L. 104-191, § 1178(b)
[5] Required by law is interpreted to mean a mandate contained in law that compels a covered entity to make a use or disclosure of PHI and that is enforceable in a court of law. (See, 65 FR 82497)

limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions[6]. (§164.512(b))

- HIPAA allows a covered entity to disclose PHI to a Health Oversight Agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight. (§164.512(d))

- HIPAA allows a covered entity to disclose PHI to the Department for the covered entity's own treatment, payment, or health care operations. (§164.506(c))

- HIPAA allows a covered entity to disclose PHI to the Department for a research study with either an authorization from the data subject or a waiver of authorization from an Institutional Review Board or privacy board. (§164.512(i))

- HIPAA allows a covered entity to disclose PHI to the Department with a valid authorization. (§164.508)

A third area of potential confusion involves when the Department must enter into a business associate agreement. A business associate agreement is only required when there is a business associate relationship, which arises when any person (including an organization) performs a function or activity that involves PHI for a covered entity or that provides a service that involves PHI to a covered entity[7]. A business associate agreement is not required for all exchanges of PHI. The business associate analysis must consider whether any persons are business associates of the Department or whether the Department is a business associate of any other covered entity. Summarized below are issues relating to business associates and the Department:

- Only the covered components of the Department will be required to determine if they have any business associates, as non-covered components are not required to enter into business associate agreements. Non-covered components, however, are required to enter into confidentiality agreements where confidential information is provided to or created by the entity with which it is contracted.

- Disclosures between a covered entity and a health care provider concerning the treatment of an individual are excluded from the requirement to have a business associate agreement.[8] For example, a business associate agreement is not

[6] The permitted disclosure of PHI authorized under state public health laws is interpreted broadly and is not to limit the authority, power or procedures established under any state or federal law. The preamble to the privacy rule provides that "procedures" authorized by law is interpreted to include State administrative regulations and guidelines. (See, P.L. 104-191, § 1178(b) and 64 FR 59998.
[7] 45 CFR 160.103 (business associate definition)
[8] 45 CFR 164.502(e)(1)(ii)(A)

required for the disclosure of PHI from a provider to a reference laboratory for the treatment of the individual.[9]

- Generally, the Department is not a business associate for its vendors. The Department does not perform a function or activity on behalf of or provide a service to its vendors. Where the program is a covered component, a vendor may very well be the Department's business associate.

- The Department is not a business associate for its licensees or other entities for which it performs a health oversight function. The Centers for Medicare & Medicaid Services (CMS) concluded that surveyed entities do not need to execute a business associate agreement with health oversight agencies.[10]

- The Department is not a business associate for entities required or authorized by law to report PHI to the Department's registries or surveillance programs.

If you have any questions about your organization's relationship with the Department regarding HIPAA, please call (617) 624-6194 and your question will be directed to the appropriate person.

[9] OCR HIPAA Privacy, December 3, 2002, Implementation Guidance at pp. 41-42.
[10] March 14, 2003 letter from CMS to State Survey Agency Directors